Opening Statement of Chairman Greg Walden
Subcommittee on Oversight and Investigations
Hearing on "Identity Verification in a Post-Breach World"
November 30, 2017

(As prepared for delivery)

Today's hearing is about the future of digital commerce. It is about the future of how we ensure the person on the other end of an online transaction is, in fact, the person they claim to be. For years, we have relied on user names, passwords and knowledge-based questions to confirm a user's identity. It's not a particularly sophisticated process – your mother's maiden name, or the make and model of your first car aren't exactly reliable forms of verification.

Regardless, this process was suitable for a period of time in the evolution of our connected world – but that time has long-since passed. As noted by one of our witnesses, it was almost a decade ago that the 2008 Commission on Cybersecurity for the 44th Presidency highlighted identity as frequent attack vector for cyberattacks.

This prompted the previous administration to launch the National Strategy for Trusted Identities in Cyberspace [N-STIC]. As we will hear today, this high-level federal attention encouraged some progress but we have a long way to go. How far? Well, according to Verizon's annual Data Breach Investigation Report, more than 80 percent of breaches last year used identity as a point of compromise.

What has changed to make existing identity management practices so ineffectual and vulnerable to attack? There are a number of factors at play but the underlying answer is fairly simple – today, the information necessary to compromise identity is readily available to those who wish to find it.

We live in a post-breach world. Just look at the massive breaches that have occurred over the last several years from Target and Home Depot to Yahoo, Anthem, OPM, Equifax and most recently Uber – to name a few. I would be surprised if anyone is this room has not had at least some portion of their personal details stolen in the last two years, let alone through their digital lifetime.

It is not, however, just stolen data the undermines current identity verification practices. The explosion of social media is also a factor. Every day consumers

voluntarily post, tweet, and share details about their lives – adding to the rich data set of information available to malicious actors.
One of our witnesses, Mr. Hunt, is a global expert on these issues – especially how bad actors can compromise identity through the collection of personal information and data that already exists in the digital universe. He endured a 27-hour journey to be here today and I suspect his testimony will be illuminating for all of us.

We can no longer ignore the current reality. Whether through theft, or voluntary disclosure, our information is out there. And this is not likely to change. Social media will continue to grow – the social, cultural and economic benefits are too great. Likewise, digital commerce and online transactions are integral to our economic prosperity – both now and in the future. As our lives become increasingly entwined with the digital space, this must come with an acceptance that our information will always be at risk.

Such is the nature of the cyber threat. There is no perfect security in the connected world, but that makes it even more important that we find ways to reduce vulnerabilities in our digital ecosystem. Clearly, identity is one of those weaknesses and I look forward hearing from all our witnesses about what options exist to address this challenge.